NASA Process Based Mission Assurance

# Enhanced Security Work Groups

## TERMS OF SERVICE

## Section 1: Enhanced Security Work Groups

Enhanced Security Work Groups (ESWGs) are available as a core functionality of the Process Based Mission Assurance (PBMA) Knowledge Management System. These ESWGs provide multi-dimensional, collaborative functionality to support the NASA Safety and Mission Assurance community, and individual program/project teams as well as formal and informal groups of subject matter experts.

## Section 2: Enhanced Security Work Groups for Sensitive Data

Enhanced Security Work Groups are also available for those that have a need to handle sensitive information, such as ITAR/EAR, source evaluation board (SEB), proprietary, and mishap investigation data (also known within NASA as Sensitive But Unclassified (SBU) data). Membership in these ESWGs are limited to those individuals involved in making NASA programs and projects successful, including contractors, industry partners, and academia. Please note: in order to set up an ESWG to handle SBU data, there are additional steps to be taken (see Section 5 below).

**Legal/Security Ground Rules:**

- **No classified information.**
- **ESWG members must be verified by their Work Group Founder.**

## Section 3: Enhanced Security Work Group Founder Requirements

The ESWG Founder is the individual (NASA civil servant or contractor) accountable for reviewing and protecting the data available on the ESWG site.

## Section 4: Enhanced Security Work Group Founder Responsibilities

For all ESWGs, the ESWG Founder is responsible for:

- Reviewing the information content of the community space to ensure the ESWG is not violating NASA policies regarding information security and technology transfer.
- Managing and controlling ESWG membership and access.
- Notifying new members that join the work group of their responsibilities.
- Visiting the community space on a regular basis, adding new information, and updating or removing old information.
- Mentoring new members in the general functioning of their community.
- Preparing a concise ESWG statement of purpose (two or three sentences).

## Section 5: SBU Enhanced Security Work Group Founder Responsibilities

In addition to the responsibilities in Section 4, each Founder of an ESWG set up to handle SBU data must:

- Complete a NAC Verification form to be authorized as an ESWG Founder per the *ESWG New User Authentication and Activation Plan.*

- Read the ESWG System's IT Security documents and sign the Data Owner's Acceptance form found in the Work Group Founders ESWG, which acknowledges that you have read and understood the security limitations and residual risks in the ESWG. Upon requesting a new SBU ESWG, your account will be added to the Work Group Founders ESWG for access to the IT Security documents and the Data Owner's Acceptance form.
- Ensure appropriate work group member access or restrictions to all SBU information in accordance with NPR 1600.1, *NASA Security Program Procedural Requirements.*
- Ensure that no administrators of the ESWG are "Foreign Persons," verifying "U.S. Person" status of each administrator through direct inquiry or other appropriate means.
- Ensure appropriate work group member access or restrictions to all SBU data, including proprietary or competition sensitive information.

## Section 6: Enhanced Security Work Group Member Requirements

The ESWG Member is any individual accessing any ESWG site.

## Section 7: Enhanced Security Work Groups Member Responsibilities

For all ESWGs, each Member must:

- Not divulge your password to anyone else. The account username and password are for your own use only.
- Not use any automatic method (e.g., sign on scripts) to gain access to the ESWG.
- Not write your password down and leave it accessible to other persons. This includes highly visible areas such as a desk or terminal, or any other location that someone could gain knowledge of your password.
- Use strong passwords, as defined by NPR 2810.1A, *Security of Information Technology*.
- Contact your ESWG Founder or Administrator if your mailing address, telephone number, employment status, or requirement for access to ESWG changes.
- Understand that information contained within the ESWG can be considered sensitive. Sensitive printed or digital media that is removed from this system must be treated in accordance with NPR 1600.1, *NASA Security Program Procedural Requirements*.
- Review the community-specific charter and any rules of engagement posted to the community space.
- Provide a biographical sketch for posting in the community space.
- Comply with these Terms of Service. Prohibited activities that are grounds for termination of participation include:
    - Violating the NASA policies regarding information disclosure.
    - Violating the NASA policies regarding security and personnel safety.
    - Using the community space for unprofessional means (e.g., spamming and flaming).

## Section 8: Enhanced Security Work Group Support Activity

- Periodic workshops will be conducted providing lessons learned and best practice case studies for ESWG Founders.
- General metrics, such as number of members and last date of activity within an ESWG, will be collected and reported to PBMA management.

Last modified: November 2007